JOINT TECHNICAL ARCHITECTURE - AIR FORCE

Air Force Enterprise Network Management Architecture Annex

27 March, 2000

Version 1.0

The Air Force Communications Agency Directorate of Global Connectivity

(HQ AFCA/GC)

SECTION 1. INTRODUCTION

1.1. ARCHITECTURES

In the world of Information Technology (IT), the term architecture can be applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a network. A technical architecture is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

The Department of Defense (DoD) Joint Technical Architecture (JTA) provides the minimum set of standards that, when implemented, permits the flow of information in support of the warfighter.

The Joint Technical Architecture – Air Force (JTA-AF) complies with the DoD JTA while providing additional guidance for Air Force systems. The JTA-AF provides corporate direction on the use of IT to support Air Force missions. The JTA-AF provides a means to increase interoperability and cost-effective sharing of information. One portion of the JTA-AF is the Fixed Base Technical Architecture (FBTA).

The FBTA defines a minimum set of technical rules, constraints, and preferences to ensure Air Force information systems implemented in the fixed base environment meet Air Force, DoD, and Joint requirements for performance and interoperability. The FBTA will eventually be replaced by several technical architectures (e.g., Information Protection, Metropolitan Area Network, and Local Area Network).

This architecture, the Network Management Architecture (NMA), addresses the network management portion of the FBTA.

1.2. NETWORK MANAGEMENT

Network Management (NM) is the execution of the set of functions required for planning, allocating, deploying, coordinating, monitoring and controlling the resources of a common infrastructure network. This execution includes performing functions such as initial network planning, frequency allocation, and pre-determined traffic routing to support load balancing, configuration management, fault management, security management, performance management, and accounting management.

1.2.1. Air Force Enterprise Network Management

AF Enterprise NM entails the management of all elements supporting those portions of the seven-layer Open System Interchange (OSI) model as seen in Table 1-1. The AF enterprise management also consists of the management of those services supporting voice, video, imagery, and sensory systems and core services supporting one network infrastructure. The AF enterprise network is managed by network control organizations organized into a tiered hierarchy.

Table 1-1 OSI Seven Layer Model

Layer	Name / Function
7	Application Layer: This layer handles issues like network transparency, resource allocation and problem partitioning. The application layer is concerned with the user's view of the network (e.g. formatting electronic mail messages). The presentation layer provides the application layer with

Table 1-1 OSI Seven Layer Model	
Layer	**Name / Function**
	a familiar local representation of data independent of the format used on the network.
6	Presentation Layer: Performs functions such as text compression, code or format conversion to try to smooth out differences between hosts. Allows incompatible processes in the application layer to communicate via the session layer.
5	Session Layer: The session layer uses the transport layer to establish a connection between processes on different hosts. It handles security and creation of the session. The presentation layer uses it.
4	Transport Layer: The transport layer determines how to use the network layer to provide a virtual error-free, point-to-point connection so that host A can send messages uncorrupted and in the correct order to host B. It establishes and dissolves connections between hosts. The session layer uses it.
3	Network Layer: The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is Internet Protocol (IP).
2	Data Link Layer: This layer splits data into frames for sending on the physical layer and receives acknowledgement frames. It performs error checking and re-transmits frames not received correctly. It provides an error-free virtual channel to the network layer. The data link layer is split into an upper sub layer, Logical Link Control (LLC), and a lower sub layer, Media Access Control (MAC)
1	Physical Layer: This layer in the OSI seven layer model concerns electrical and mechanical connections and MAC. The data link layer uses it. Example physical layer protocols are Carrier Sense Multiple Access / Collision Detect (CSMA/CD), token ring and bus.

Table 1-1. OSI Seven Layer Model

1.2.2. AF Tiered Network Control Organizations

Each AF network control organization is assigned to one of three tiers (see Figure 1-1), each with its own area of responsibility (AOR). These organizations, tiers, and AORs are:

AF Enterprise Network Operations Organization	Tier	AOR
Air Force Network Operations Center (AFNOC)	1	Air Force
Network Operations and Security Center (NOSC)	2	MAJCOM
NOSC-Deployed (NOSC-D)	2	NAF
Network Control Center (NCC)	3	Wing
NCC-Deployed (NCC-D)	3	Wing

See Appendix 2 for a complete description of each network control organization.

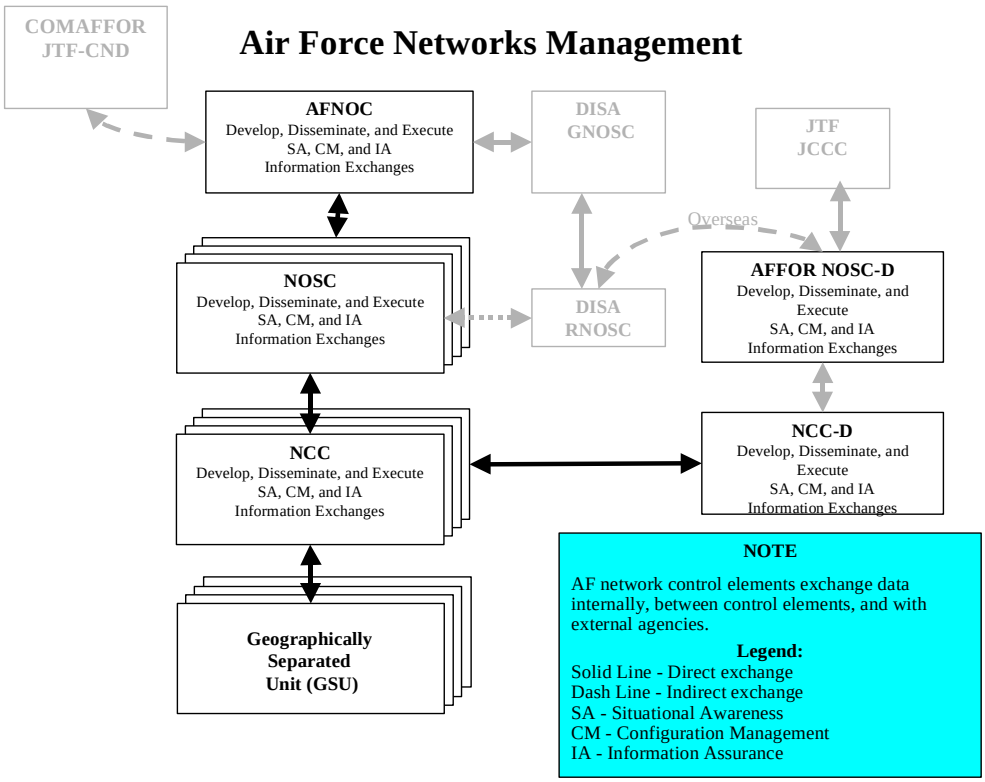

Figure 1-1. AF Enterprise Network Management

1.2.3. Air Force Network Management

Air Force NM describes proactive and reactive operations performed by the AFNOC, NOSCs, and the NCCs. Timely execution of standard NM operations across the 3-tiered Air Force enterprise network enables the AFNOC, NOSCs and NCCs, to defend, control, manage, modify, and monitor their respective voice, video, imagery, data, and sensor networks in a complimentary and uniform manner. To achieve the goal of network management, this network management architecture has been developed.

1.3. NETWORK MANAGEMENT ARCHITECTURE (NMA)

The NMA provides a baseline that addresses issues used to define the AF enterprise NM operations in terms of Operational, Technical, and System Architectures. This architecture describes functional areas, components, standards, and the solutions using AF-preferred procedures, hardware, and software. The NMA also maps the operational, system, and technical architectures into a uniform business process of conducting AF enterprise network operations--to include the fault, configuration, accounting, performance, and security (FCAPS) network management functions (see Appendix 3). The application of this architecture mandates the execution of FCAPS functions using the standard AF Combat Information Transport System (CITS) Network Management System/Base Information Protection (NMS/BIP) components, core network services, and enterprise network operations across the AF enterprise network.

1.3.1. NMA Focus

The NMA is constructed from an Internet Protocol (IP) point of view. This architecture focuses on the data transport portion of the network. [1]

1.3.2. NMA Iteration Cycle

The NMA is reviewed and updated semi-annually.

1.3.2.1. Past NMA Iterations

This is the first iteration of the NMA.

1.3.2.2. Current NMA Iteration

This iteration of the NMA describes only the unclassified portion of the AF enterprise NM as it currently exists at main AF operating locations.

1.3.2.3. Future NMA Iterations

Future iterations of this architecture will cover:

- MAJCOM unique infrastructures (e.g., Air Force Space Command)
- How MAJCOMs and Wings support geographically separated units (GSUs)
- Classified and C2 systems
- Steps towards convergence of voice, video, imagery, data, and sensor networks
- Network Management in the deployed environment
- Non-IP voice and multimedia that ride the network

1.3.3. NMA Timeframes

All of the technical architectures, developed for the JTA-AF, have defined three time frames based on the Program Objective Memorandum (POM) cycle fiscal year 2000 (FY00). These timeframes are identified as follows:

- The "Now" architecture focuses on the FY00-FY01 timeframe
- The "Future" architecture focuses on the FY02-FY07 timeframe
- The "Strategic" architecture identifies needs from FY08 and beyond

1.3.3.1. "Now" Architecture

The "Now" architecture will concentrate on requirements in which the Air Force has a product solution identified (i.e., CITS NMS/BIP) in FY00 through FY01.

---

[1] See Voice Switching Systems and Multimedia architectures for information on Non-IP voice and multimedia.

1.3.3.2. "Future" Architecture

The "Future" architecture will focus on solutions advancing towards the goal of migrating voice, video, and data onto a single transport mechanism. For this iteration, Section 6 lists some general areas to consider, as well as a few classes of products that should be considered. The "Future" architecture will be addressed in greater detail in later iterations of this architecture.

1.3.3.3. "Strategic" Architecture

The "Strategic" architecture will present the visionary architecture required to achieve Joint Vision 2010 goals. The "Strategic" viewpoint will be covered in greater detail in later iterations of this architecture.

1.4. NMA SCOPE OF OPERATIONS

The AFNOC, NOSCs, and NCCs work in unison to manage all components and services in the aggregate AF enterprise network. Figure 1-1 illustrates the scope of AF enterprise NM operations. Figure 1-2 illustrates the scope of operations for a typical base-level NCC, which manages those items below the dashed line. AF NM entails the management of all network elements supporting active Wing, MAJCOM, and AF enterprise data networks. Other elements supporting voice, video, imagery, and sensor systems will be incorporated in a later iteration of this architecture. NM functions in support of tenant units are delineated in a Service Level Agreement (SLA) in accordance with AFI 33-115 V1.

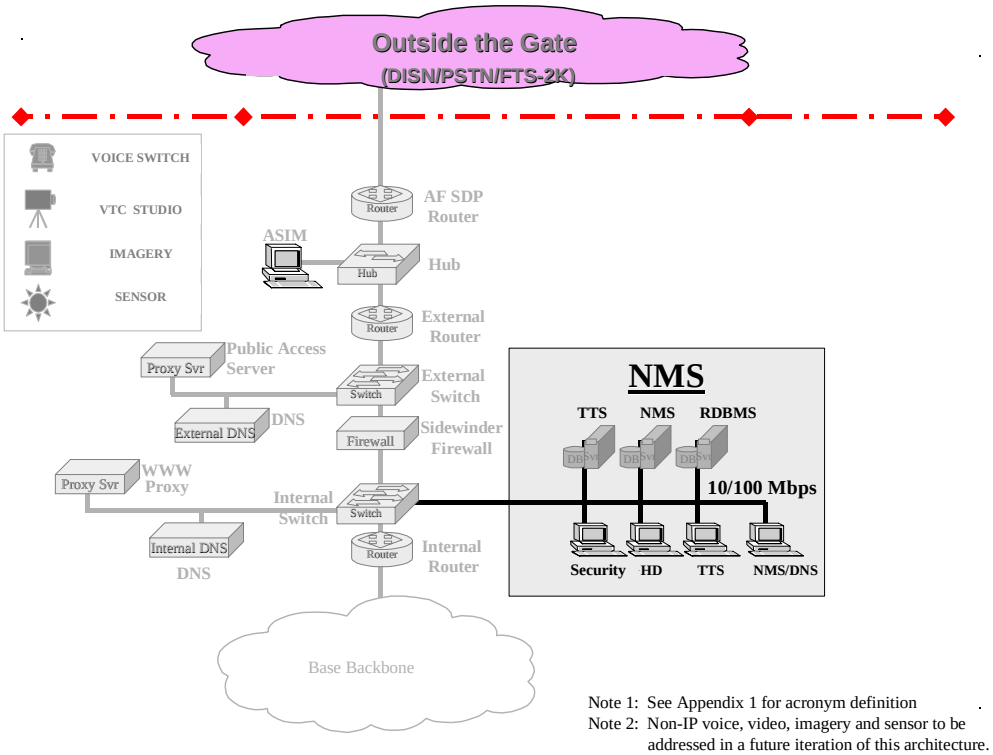

Figure 1-2. "Now" AF Base-level Network Control Center

1.5. NMA NETWORK OPERATIONS GOAL

The NMA end-state goal is to provide the AFNOC, NOSCs, and NCCs with a standard NM guidance from which they can conduct essential NM operations. To accomplish this, the AF employs a standard set of NMS/BIP tools at the AFNOC, NOSCs, and NCCs. These tools form the foundation from which AFNOC, NOSCs, and NCCs execute AF enterprise NM operations. The BIP portions of this tool set are documented under the Information Protection Architecture. The NMS tools, their configuration, and usability to conduct FCAPS management operations are documented in this architecture. Architecture integration relies heavily on automatic and manual process interaction occurring between the NMS and BIP components.

1.6. NMA IN THE GLOBAL INFORMATION GRID – AIR FORCE

The Global Information Grid-Air Force (GIG-AF) is the system of globally interconnected capabilities, associated processes, and personnel that collects, processes, stores, disseminates, and manages information used by warfighters, policy makers and support personnel. The GIG-AF consists of four segments: Outside the Gate, Inside the Gate, Last 400 Feet, and Information Appliances, as seen in Figure 1-3. The figure shows NM as part of the Inside the Gate portion of the GIG-AF, but NM actually reaches into all segments of the GIG-AF. Nevertheless, this iteration focuses primarily on the Inside the Gate portion of NM.

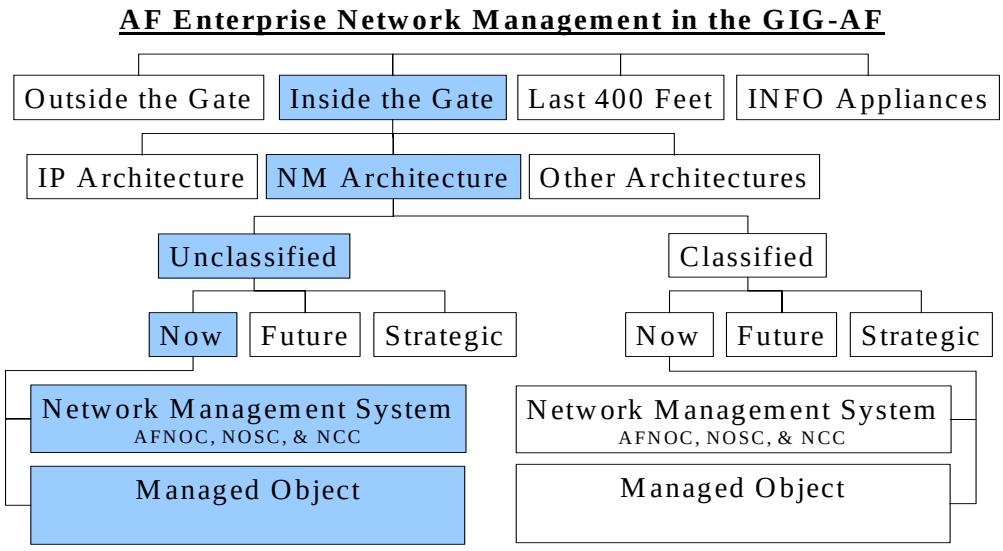

Figure 1-3. NM in the Global Information Grid – Air Force

SECTION 2. FUNCTIONAL AREA DESCRIPTIONS

This section describes the functional areas chosen as the foundation for AF enterprise network management. Although the initial iteration of this architecture focuses on network management of unclassified data networks, these functional areas are based upon industry standards and are applicable across the entire spectrum of network management.

The AF enterprise NM operations are grouped according to the five NM functions as defined in the *International Standards Organization/International Electro-technical Commission (ISO/IEC) Joint Technical Committee Open System Interconnection Reference Model Part 4: Management Framework (IS 7498-4)*. The NM functional areas are fault, configuration, accounting, performance, and security (FCAPS) management. Descriptions are provided in subsequent paragraphs.

2.1. FAULT MANAGEMENT

Fault Management (FM) encompasses fault detection, isolation, and correction of abnormal operation of the Open System Interconnect Environment (OSIE). Faults cause open systems to fail to meet operational objectives and may be persistent or transient. Faults usually expose themselves in the form of hardware and/or software errors and error detection capabilities can recognize those faults. FM functions include:

- Provide automated trouble ticketing
- Maintain and examine error logs
- Accept and act upon error detection notification
- Trace and identify faults
- Perform a sequence of diagnostic testing
- Correct faults
- Poll managed devices
- Provide automated recovery and backup of managed devices (i.e. configuration restoral)

2.2. CONFIGURATION MANAGEMENT

Configuration Management (CM) identifies, exercises control over, collects data from, and provides data to open systems. It does this to initialize, start, provide for the continuous operation of, and terminate interconnection services. CM functions include:

- Set parameters that control routine operations of an open system
- Associate a name with a managed object and sets of managed objects
- Discover, determine, map, and record network components, applications, and configurations (hardware & software)
- Initialize and shut down managed objects and connections
- Collect information on demand concerning current status of an open system
- Receive notifications of significant changes in the condition of an open system

- Change the open system's hardware and software configuration (e.g., additions, deletions, and changes)
- Collect system administrator data, system's mission, device criticality, and device sensitivity

2.3. ACCOUNTING MANAGEMENT

Accounting Management (AM) enables charges to be established for the implementation of OSIE resources and for the costs to be identified for the use of those resources. AM functions include:

- Inform users of costs incurred or resources consumed
- Enable accounting limits to set and tariff schedules to be associated with the use of resources
- Enable costs to be combined where multiple resources are invoked to achieve a given communication objective
- Collect customer traffic statistics
- Display and print real-time analysis of interface related data and reports

2.4. PERFORMANCE MANAGEMENT

Performance Management (PM) evaluates the behavior of OSIE resources and the effectiveness of Communication and Information (COMM & Info) interconnections. PM functions includes:

- Gather statistical information; establish baseline of normal behavior
- Maintain and examine error logs of systems and state histories
- Determine system performance under natural and artificial conditions
- Alter system modes of operation for the purpose of conducting performance management activities
- Sample critical performance parameters
- Produce trend analysis reports and graphs
- Sort and file network traffic data based on source and destination IP addresses

2.5. SECURITY MANAGEMENT

Security Management (SM) is performed using Base Information Protection (BIP) tools and is documented in detail in the Information Protection architecture. A general description is provided here for informational purposes only. Security management provides boundary protection, intrusion/misuse detection, internal control, access preservation, authentication and encryption, backup, and recovery. BIP must monitor, deter, detect, isolate, contain, control, report, and recover from intentional or unintentional unauthorized intrusions, abuse, denial of service, and use of Automated Information System (AIS) resources. SM functions include:

- Creation, deletion, and control of security services and mechanisms
- Distribution of security-relevant information
- Report of security-relevant information

SECTION 3. ARCHITECTURE DESCRIPTION

The AF NMA is comprised of two distinct sub-architectures, the Network Management System (NMS) and Managed Objects. The NMS components host NM manager applications that monitor and control managed objects. The NMS supports AF network management operations within a specific area of responsibility (AOR) by using virtual private network (VPN) technology. The Managed Objects sub-architecture consists of all the managed networked components--hardware and software, including NMS components themselves--within a particular network control organization's AOR. Every managed object hosts a NM agent that is monitored or controlled by a NM manager application.

Figure 3-1 illustrates that each FCAPS functional area interacts with and depends on actions occurring between the NMS and Managed Objects components. The NMS system design integrates the interactions using expert rules, scripts, and necessary information exchanges.

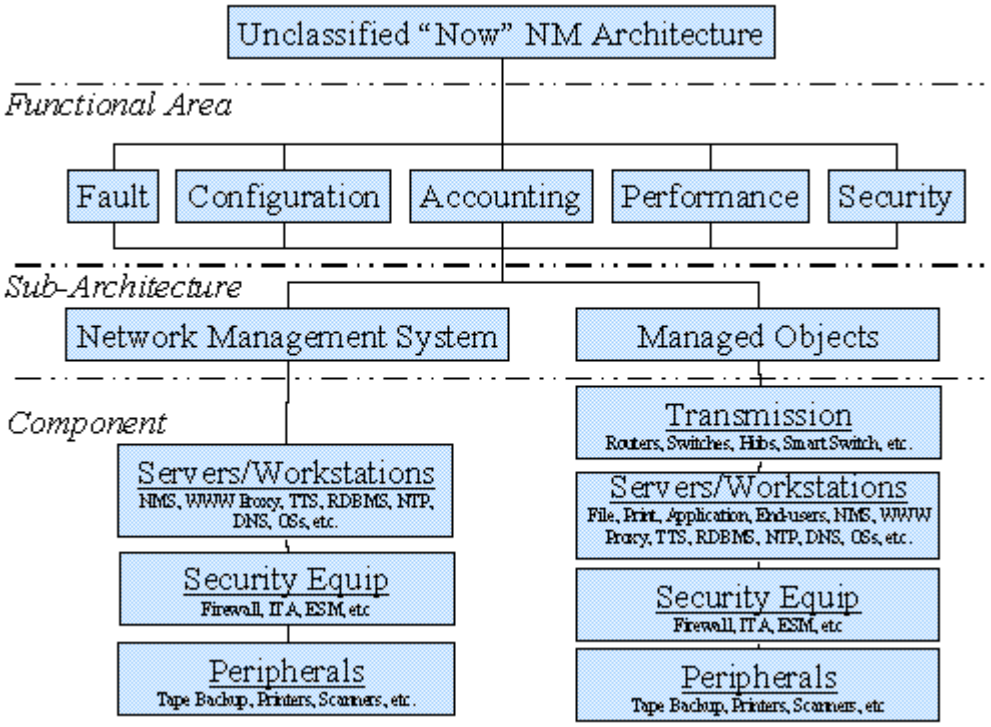

Figure 3-1. Functional Area, Architecture, and Component Relationships

Interaction between the NMS and Managed Objects sub-architectures and with the Information Protection Architecture is crucial. Details on information protection components can be found in the Information Protection Architecture. An explanation of the NMS and Managed Objects sub-architectures follows.

3.1. NETWORK MANAGEMENT SYSTEM (NMS)

Figure 3-2 illustrates the standard AF NMS architecture that is employed at each NCC and at the AFNOC. The AF NMS's applicability to support NOSC NM operations is under review.

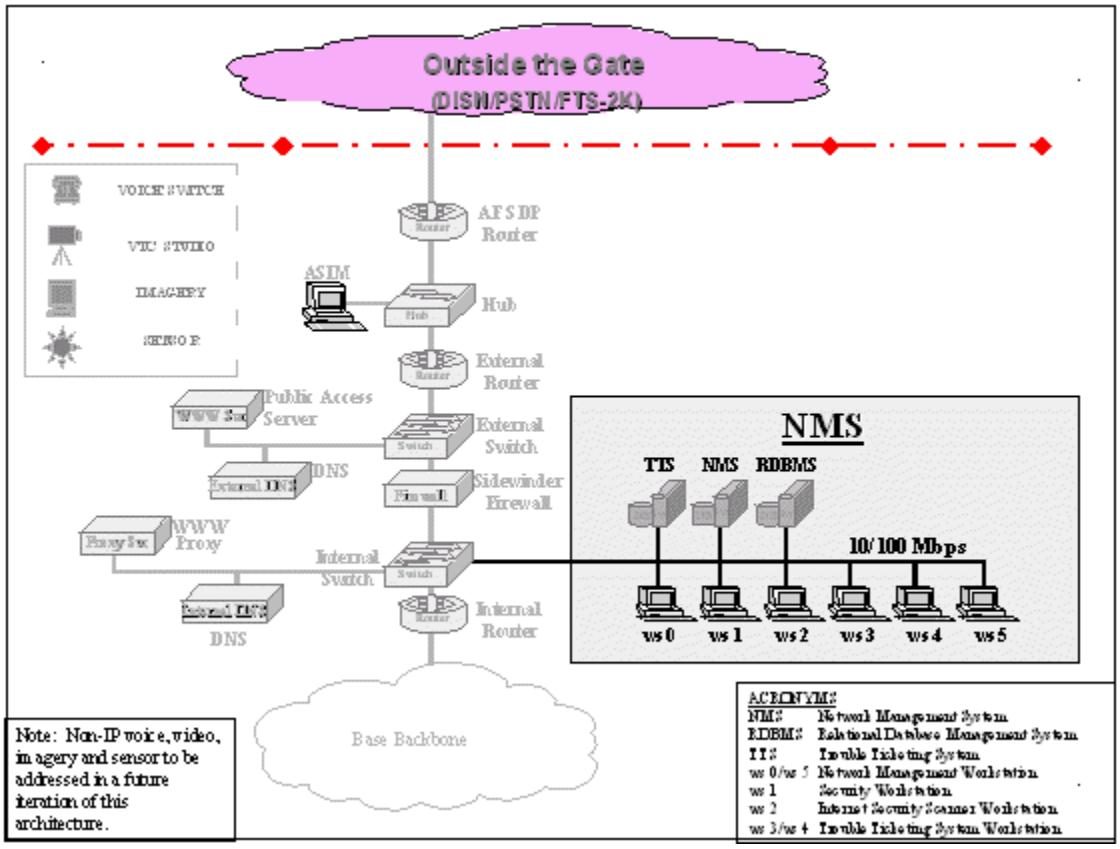

Figure 3-2. NMS in the AF Enterprise Network

3.1.1. NMS Implementation

The AFNOC, NOSCs, and NCCs implement the NMS architecture in order to conduct AF enterprise network operations and network management services. The NMS components work in unison to provide the capabilities to conduct FCAPS management functions.

3.1.2. Scope of NMS Tool Set

The standard NMS tool set must be compatible with multi-vendor operating systems/equipment and must provide total management of all data network components. It must manage the information transport system components.

3.1.3. NMS Capability

The NMS capability must support the data networks within enclaves at each level of classification on the base (i.e., sensitive but unclassified, Secret, etc.). Management and protection must take place in each of the corresponding data "streams" because the data at various classification levels is separated either physically (completely parallel networks) or logically (with the use of virtual private networks using in-line encryption).

3.2. MANAGED OBJECTS

Managed objects are those devices or applications that can be monitored or controlled by an NMS component. Although there may be some commonality, managed objects will vary from site to site depending upon what hardware and software is installed. In the initial iteration, the focus of managed objects will be establishing control of items common to most sites, that is the NMS/BIP and Information Transport System (ITS) components installed under an ongoing infrastructure modernization program.

3.2.1. Network Management in Area Networks

The NM aspects associated with managed objects which reside within the Wide Area Network (WAN), Metropolitan Area Network (MAN), and Local Area Network (LAN) architectures are described below. Other aspects of the WAN, MAN, and LAN architecture components are documented in their respective architectures. The reader should consult those architectures for details.

3.2.2. Network Management Agents

The NMS system conducts FCAPS functions to monitor and/or control the various managed objects. An agent (software) typically resides on each managed object. The agent responds to commands and information requests from specific NMS manager applications. The agent may also be configured to automatically notify the NMS manager of specific conditions. The agents typically use standard management information base (MIB) objects to store information. These MIB objects are sanctioned by the Internet Engineering Task Force (IETF), although some managers and agents support vendor specific extensions. Remote Network Monitoring (RMON) MIB objects are the most prevalent. Communication between the NMS manager and the agent is typically via the Simple Network Management Protocol (SNMP).

SECTION 4. COMPONENT, SERVICE, AND "NOW" SOLUTION

This section covers the components, services, and "Now" solutions of the NMA and its sub-architectures. Components are the hardware and software necessary to provide network management capabilities. Services are the functional subsets of each component. Because of the tight integration of the components and their respective subsets, both are covered in this section. Where applicable, detailed discussions of a component's subsets are included.

4.1. AF STANDARD NMS

Interaction and information exchange between the individual NMS and BIP components, and between the NMS systems located at the AFNOC, NOSCs, and NCCs, are crucial to conduct complete, effective AF enterprise network operations. The AF standard NMS/BIP design combines individual components into a single system that provide FCAPS functions. The AF-standard NMS is currently fielded at all NCCs and the AFNOC; its applicability to support NOSC NM operations is under review.

The following NMS components have been installed, or are scheduled for installation, at all AF bases under an ongoing infrastructure modernization program.

- Hewlett Packard (HP) OpenView (OV) for Windows NT
- CiscoWorks for Windows NT
- Dolch PAC64/Network General Protocol Analyzer
- Legato Network and Exabyte Mammoth
- Spectracom Master Clock and GPS Receiver
- Servers and Workstations: Based on Windows NT server and workstation OS
- DNS/IP Management - Enterprise License for Lucent's QIP product
- Trouble Ticketing System (TTS) - Enterprise License for Remedy Trouble Ticketing License, includes
    - Remedy Action Request System (ARS)
    - Remedy Distributed Server Option (DSO)
    - Remedy fixed/floating client licenses
- Microsoft SQL Server

4.2. NMS FCAPS FUNCTIONALITY

The NMS hardware and software components, along with their respective FCAPS functionality, are described in the remainder of this section. NMS components will be described first, followed by description of the managed objects. Component descriptions include: NMS Server, NMS Workstations, NMS Applications, External Router, External Switch, Firewalls, Internal Switch, Domain Name Service Servers, Remote Access Server, WWW Public Access Server, Caching Proxy Server, and NTP Server.

4.3. NMS COMPONENTS

Looking at Figure 3-2, the NMS components are contained in the shaded NMS box. The following paragraphs describe these components and their relationships to the FCAPS functional areas. Note that some of these components overlap functionality with Information Protection Architecture components. For those components, refer to the Information Protection Architecture for additional information.

4.3.1. NMS Server

The Network Management Server contains a suite of network management and information protection applications. The minimum hardware configuration of the NMS server is a 450 MHz Pentium class server with 566 Mb of memory, three 4.3 GB Dual Channel Wide Ultra SCSI-3 hard drives with RAID (Redundant Array of Inexpensive Disks) 5. The server runs Windows NT v4.0 with Service Pack 3. The NMS server hosts HP OV NNM, and CiscoWorks for NT. Full FCAPS functionality provided by the NMS components is used to manage the NMS server. The server performs the following functions:

- Network Mapping
- Fault Detection
- Limited Fault isolation
- Limited Performance Monitoring
- Forward Critical Node Alerts to TTS

4.3.2. NMS Workstations

The first three workstation descriptions below were installed at all AF bases with the initial standard NMS design and are designated as ws0, ws1, and ws2 respectively. The next three workstation descriptions are associated with the follow-on AF standard NMS design and are designated as ws3, ws4, and ws5 respectively. The follow-on effort is in-progress, and is projected to install these workstations at all AF bases by FY01. Each workstation is configured to serve multiple purposes as described below. Full FCAPS functionality provided by the NMS components is used to manage the NMS workstations.

4.3.2.1. Network Management Workstation (ws0)

The Network Management Workstation (ws0) hosts HP OV Remote Console Application, CiscoWorks for Win NT 4.0 Server, Win NT 4.0 Server with Service Pack 3, and Legato Administration Server. PowerChute Plus is installed to manage the Uninterruptible Power Supply (UPS) connected to the workstation.

4.3.2.2. Security Workstation (ws1)

The Security Workstation (ws1) contains the Graphical User Interface (GUI) of Axent's OmniGuard Intruder Alert (ITA) and Enterprise Security Management (ESM), HP OV Remote Console Application, PowerChute Plus, Netscape Navigator and Win NT 4.0 Server with Service Pack 3. NCC controllers use the ESM GUI to send requests to the ESM's manager and agents. They format the information for display, creating spreadsheet reports, pie charts, bar charts and other visual objects. The ESM GUI connects to other components using the Client Server

Protocol. The ITA GUI allows NCC controllers to create rules and polices via the ITA Manager and ITA. Netscape Navigator is used to manage the Netscape Proxy Server and PowerChute Plus to manage the workstation's UPS. Only this workstation is configured to administer the Netscape Administration Server.

4.3.2.3. Internet Security Scanner Workstation (ws2)

The Internet Security Scanner Workstation's (ws2) Information Protection roles are described in the Information Protection Architecture. In regards to Network Management, this workstation allows the network administrator to monitor new network nodes that come up on the network. It contains HP OV Remote Console Application and Win NT 4.0 Server.

4.3.2.4. Trouble Ticketing System Workstation (ws3 and ws4)

The Trouble Ticketing System (TTS) Workstations (ws3) and (ws4) minimum hardware configuration consists of 400 MHz Pentium class workstation with 128 MB RAM, 9.1GB Wide Ultra SCSI hard drives, and 17 inch monitors. Software includes the Remedy ARS, Flashboards, Legato clients; PowerChute PowerNet Agents; MS Internet Explorer; MS Exchange clients; and Windows NT workstation 4.0.

4.3.2.5. Network Management Workstation (ws5)

The Network Management Workstation (ws5) hosts HP OV NNM client, CiscoWorks client, Lucent QIP DNS client, ITA/ESM agents, Legato client, PowerChute Agent, MS Internet Explorer, and MS Win NT 4.0 Server with Service Pack 3. Its minimum hardware configuration consists of a 400 MHz Pentium class workstation with 128 MB RAM, 9.1 GB Wide Ultra SCSI hard drive, and a 21 inch monitor. The initial operating system is Win NT Workstation 4.0 with Service Pack 3. The Network Management Workstation functions as the HP OpenView manager/collector, DNS manager, and CiscoWorks manager.

4.3.3. Trouble Ticketing System (TTS) Server

The TTS Server has a minimum configuration of a 450 MHz Pentium class server with 320 MB RAM, and three 4.3 GB Dual Channel Wide Ultra SCSI-3 hard drives with RAID 5. Software includes ARS Server, Remedy Distributed Server Option (DSO), and Remedy ARS Clients, running on Win NT 4.0 Server with Service Pack 3. An HP LaserJet 5 Printer enables NCC help desk technicians to print trouble tickets.

4.3.4. Relational Database Management System Server (RDBMS)

The RDBMS Server has a minimum configuration of a 450 MHz Pentium class server with 566 MB RAM, three 4.3 GB Dual Channel Wide Ultra SCSI-3 hard drives with RAID 5, and a redundant power supply, running under Win NT 4.0 with Service Pack 3. Microsoft SQL is the selected database. The data store is considered a core element of Remedy ARS. Other NMS/BIP components integrate with the database as the central data repository. Microsoft SQL Server is intended for usage only in conjunction with the Remedy ARS trouble ticketing software in the NCCs. SQL Server performs as the database engine for the trouble ticketing function.

4.3.5. DOLCH PAC 64 Protocol Analyzer

The Network General software is loaded in the DOLCH PAC 64 to provide protocol profiling and analysis. This is helpful in detecting and analyzing outgoing and incoming base traffic. This will assist administrators in configuring the router and the firewall access control lists. The protocol analyzer also diagnoses general network malfunctions in a non-intrusive manner. It assists the NCC Controllers to perform fault and performance functions of the FCAPS model.

4.3.6. HP OpenView Network Node Manager (NNM)

Network Node Manager performs fault, configuration, and performance management function of the FCAPS model for multi-vendor Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NNM can automatically: discover the network environment and monitor its status; draw IP or Internet Packet Exchange (IPX) topology maps based on discovered information; manage any vendor device that supports the Simple Network Management Protocol (SNMP); and diagnose network faults and performance problems from one location.

4.3.6.1. Network Status

HP OpenView NNM diagnoses problems by looking at trends over time, get and set values for Internet management information base (MIB) objects using a point and click operation, and builds new MIB applications without programming for Internet-standard and enterprise-specific MIBs. The NNM collects historical MIB information about MIB objects, stores MIB data for trend analysis, graphs collected data, and defines event thresholds for MIB objects. It can define actions to be taken upon receipt of a SNMP or Desktop Management Interface (DMI) event.

4.3.6.2. Network Node Manager Operations

Vendors MIB variables are loaded into NNM upon installation to accommodate NM metrics collection and processing and device reconfiguration. The firewall configuration must allow SNMP, Internet Control Message Protocol (ICMP), and SNMP-Traps either by the use of proxies or an IP filter between the NMS and the managed objects in a bi-directional manner. (Refer to the Information Protection Architecture for details on use of ICMP and SNMP.) Initially, the following critical network components are managed:

a) Network connectivity devices: Repeaters, Bridges, Routers

b) Network Servers: UNIX, Windows NT and Novell

c) Additional SNMP manageable devices such as UPS and firewall SNMP Traps

4.3.6.3. NNM Network Diagnostics

NNM provides the capability to diagnose network malfunctions non-intrusively at affected network segments. NNM represents managed objects by symbols, while the object's status is represented by different colors. NNM is not responsible for objects not selected by the operator or objects that do not support SNMP. NCC controllers manually add the external router, the external switch and any other devices external to the firewall that will be managed by NNM.

4.3.7. CiscoWorks

CiscoWorks is a management platform for managing Cisco-based enterprise networks and devices. This product provides inventory, configuration, and software management capabilities;

traffic management tools; as well as integrated views and reports of network information. CiscoWorks Windows is a suite of GUI-based device management applications that run on Windows NT. CiscoWorks Windows provides dynamic status, statistics, and comprehensive configuration information for Cisco devices. CiscoView manages Cisco routers and switches through SNMP. Applications available with CiscoView include Threshold Manager, StackMaker, Flash File System, and AS 5200 Manager. Descriptions of each follow:

4.3.7.1. CiscoWorks Threshold Manager

Threshold Manager allows you to set thresholds and retrieve event information. Threshold Manager relies on Remote Network Monitoring (RMON) alarm and event groups supported in Cisco routers and switches. Threshold Manager is a CiscoView-launched threshold management application. It provides an easy-to-use GUI that NCC Controllers use to set thresholds on network devices using Cisco-provided, predefined default policies. A policy is a set of predefined configuration information that specifies the condition for triggering a threshold event. Policies can be applied automatically to target devices. It can also retrieve event information from devices. Threshold Manager also supports detailed customization of threshold settings. Version TMNT95 supports Windows NT 4.0.

4.3.7.2. CiscoWorks StackMaker

StackMaker manages the device membership in a Cisco stack. It is an application that works with the CiscoView software to provide enhanced manageability for devices. StackMaker enables you to display a set of individual, stackable devices and create a stack containing these devices. Devices supported by StackMaker include the Catalyst 1900, Catalyst 2800 and the Catalyst 2820.

4.3.7.3. CiscoWorks Flash File System

The Flash File System provides configuration file editing and display functionality for high-end routers, Cisco 7000, 7010, 7200, and 7500 Series. The Flash File system is a tool that is used to manage flash files such as router image files and router configuration files. Each router on which flash files are maintained must be configured for flash administration.

4.3.7.4. AS5200 Manager

AS5200 Manager is a modem management application used to monitor, configure, and troubleshoot the AS5200 Access Server.

4.3.7.5. Enterprise NM Controllers

Enterprise NM Controllers modify the SNMP Community strings to comply with the Air Force Bases' Standard Operating Procedure.

4.3.8. Remedy Action Request System (ARS) Trouble Ticketing System (TTS)

Remedy ARS is the main Automated Trouble Ticket/Help Desk GUI user interface to the NMS/BIP. The two servers that support the ARS TTS are described below. ARS provides a general service request function. User requests and problems are entered and tracked through the system. An expert relational database management system (RDBMS) containing problem

solutions is created as resolved trouble/problem information is entered into the system. This Microsoft SQL 7.0 database becomes an AF-wide resource of vital information that streamlines processes, answers questions, reduces support staff burden, tracks man-hour expenditures, and eliminates the need to recreate existing solutions.

4.3.8.1. Remedy ARS Centralized Management

Remedy's ARS supports the three-tiered client/server architecture. The centralized management system is designed to isolate and react to network faults before fatal system errors occur. Users of the ARS TTS Group List can be an assigned technician and/or an assigned manager. The ARS is flexible in that it is database, hardware, and operating-system independent. It is scaleable to meet changing organizational needs from small to multi-site, global implementations.

4.3.8.2. ARS Support Components

NCC controllers use the ARS TTS components, including TTS schema and PERL scripts, to meet the fault, performance, and accounting functions of the FCAPS model. ARS provides a general service request function. User requests, as well as problems, are entered and tracked through the system. As problem resolutions are entered into the system, a separate RDBMS creates an expert set of problem solutions (a historical repository). The repository becomes an AF-wide resource of vital information that streamlines processes, answers questions, reduces support-staff burden, tracks man-hour expenditures, and promotes migration of independent self-help Help Desk (HD) solutions to AF enterprise HD operations. Users directly query the system to check for status and view a history of events without HD staff assistance or intervention. ARS standard templates can be customized to handle key areas of information management. The ARS uses five applications: AR Admin Tool, AR User Tool, AR Notifier Tool, AR Import Tool, and AR License Tool.

4.3.8.3. AR Admin Tool

The AR Admin Tool is used to control workflow by setting up the trouble ticketing tracking system database schemas. It is used to create and modify the GUI layout and definition of menu lists, filters, active links, and event/problem escalation procedures. It also provides a capability to create and modify license management, server settings, and user permissions. Primary functions include:

- Menus with pull-down values are attached to schema fields to assist users with data entry and to alleviate data entry errors.
- Schema filters test server transactions against pre-set conditions. It invokes actions (e.g., notification, problem escalation, alarm generation, alternate route establishment, etc.) in response to those conditions to guide the problem resolution process.
- Active links tie data in different database schemas together. A link is executed if a condition is met. Links perform actions such as loading data into a schema from an alternate source, running macros, displaying messages, and/or running a process.
- Event/problem escalation enables a condition to be checked on a regular basis, and informs the appropriate groups or individuals to take action. For example, event/ problem escalation could check to see if a ticket has been opened for more than 24 hours. If the condition is met, the ticket status changes and the supervisor is notified.

4.3.8.4. AR User Tool

The AR User Tool is a GUI-based tool used to *Submit*, *Modify*, *Query*, and/or *Report* events, problems, and trouble tickets. The following is a brief description of the AR User Tool functions:

- Submit enters information (e.g., trouble ticket, metric, inventory, etc.) into the ARS RDBMS.
- Query searches the ARS RDBMS for information and displays it.
- Modify updates ARS RDBMS information.
- Report queries the ARS RDBMS and sends the information to a screen, printer, file, or to other applications.

4.3.8.5. AR Notifier Tool

The AR Notifier Tool is used to generate and/or receive notifications (e.g., alarms, alerts, event/problem escalation, trouble ticket initiation, etc.) for a group and/or an individual. An administrator sets the condition parameters that initiate a notification, specifies who gets notified, and when the notification is sent. AR Notifier runs in the background as a service in the client workstation and receives notifications from the ARS server. Notification alerts are user-set and include pop-up messages, a Notifier window, flash icon, or a beep. A notification log is also available for historical reference.

4.3.8.6. AR Import Tool

The AR Import Tool is used to import/export data to or from AR Server. It is a utility program that loads data from a 3rd-party file into the ARS RDBMS. It is useful for sending and receiving information (e.g., user name, E-mail address, location, inventory, performance metrics, etc.) to other than ARS tools. It can also migrate existing help desk information into ARS.

4.3.8.7. AR Licenses Tool

The AR Licenses Tool is used to manage the three types of licenses: fixed, floating, and read. Fixed licenses enable specific individuals to process (submit, query, modify, and report) ARS RDBMS data. Floating licenses do the same thing as fixed licenses, but are not assigned to one individual at a time. Floating licenses are used on a first-come, first-serve basis. If all floating licenses are in use, other users must wait until a license becomes available before they can modify the ARS RDBMS data. An unlimited number of read licenses are available and can only be used to read and submit information.

The Air Force has a restricted enterprise license available for Remedy products. The CITS Program Management Office (PMO) acquired the enterprise licenses and are the point of contact for additional information.

4.3.8.8. Distributed Server Option

Remedy DSO enables geographically-dispersed organizations to coordinate the activities of help desks around the world. DSO routes requests among servers across the network based on factors such as time-of-day, area of expertise or functional area. Workflow-driven replication transfers the minimum amount of information between servers, optimizing Intranet bandwidth. Because DSO transfers requests immediately and transparently to the appropriate help desk organization

or individual, it promises towill assist NCCs, NOSCs, and the AFNOC to optimize AF-wide help desk resources for quick problem resolution.

4.3.9. Legato Tape Backup

Legato NetWorker provides the capability to manage, configure, and monitor network servers' tape backups. The Legato NetWorker Client software is installed on the Security Management Server and Netscape Proxy Server to provide for automated backup management from the Legato NetWorker Server residing in NMS. After loading the client software, the clients must be properly registered with the Legato NetWorker server. The Exabyte Tape Drive is used in conjunction with Legato NetWorker to manage and configure automatic backups and recovery of AF standard NMS/BIP phase 1 servers, excluding the firewall server. NCC Controllers use the Legato and Exabyte equipment to perform the backup sub-function of the security function of the FCAPS model.

4.3.10. Axent Intruder Alert (ITA)

Intruder Alert is primarily an Information Protection tool, as documented in the Information Protection Architecture. ITA monitors, detects, and responds to information system threats in real-time across the internal, distributed, base network environment. The ITA is the intelligent component of ESM that performs the actual security checks. The ITA performs all of the processing, thereby reducing network overhead traffic and the Enterprise Security Manager's processing power requirements. It detects and responds to unauthorized activity, ensures integrity and confidentiality of data, administers users and network resources, controls access to those resources, and identifies and authenticates users.

4.3.11. ITA Agent

The ITA agent software is primarily an Information Protection tool, documented in the Information Protection Architecture. Within NM, NCC Network Defense Controllers use the two tools to conduct the pertinent configuration and security functions of the FCAPS model. The tools are ITA Admin and ITA View.

4.3.11.1. ITA Admin

ITA Admin is a Windows NT application serving as the command center. It organizes managers and agents, creates and administers security policies, manages users and user privileges, and updates the manager's licensing privileges. It supports an unlimited number of managers—providing valid licenses are available. There are "out-of-the-box" security policies available for immediate use.

4.3.11.2. ITA View

ITA View is a Win NT GUI used to view event data captured by the deployed agents. ITA View enables the NCC Network Defense Controller to query the event database for conditions that triggered pre-defined security policies and/or rules, a portion of the security function of the FCAPS model. It generates reports based on queries.

4.3.12. Axent Enterprise Security Manager (ESM)

ESM is a software tool that manages and enforces security data and policies across a full range of multiple client/server platforms (e.g., Win NT, Unix, NetWare, web server, etc). It is primarily an Information Protection tool, and its full functions are documented in the Information Protection Architecture. Some of its Information Protection functions double as NM functions, primarily in configuration management. ESM determines which security policies and procedures need to be established for each resource type and then checks the resource's compliance with those policies. ESM checks system for vulnerabilities and unauthorized privileges, provides integrity checks, and detects changes to security settings or files. It receives data from the ITAs, then formats and reports the data to the NCC controller that requested the information.

4.3.13. Internet Scanner SafeSuite (ISS)

The ISS is primarily an Information Protection tool and its primary functions are identified in the Information Protection Architecture. The ISS is included here since portions of the information gathered are also valuable in the NM arena. Its comprehensive set of network vulnerability security assessment tools is designed to audit, correct, and monitor all aspects of network security. This provides essential configuration and accounting management information.

4.4. MANAGED OBJECTS COMPONENTS

Managed Objects include networked components from the AF Service Delivery Point (SDP) router, through the base backbone, to the end user desktop. Figure 3-1 illustrates various transmission components, workstations and servers (including applications), and peripherals. Figure 3-2 depicts the major managed hardware objects, in order, starting from the AF SDP router to the base backbone. The following paragraphs describe these components, and their relationships to the FCAPS functional areas.

4.4.1. DISA NIPRNET/SIPRNET Routers and IDNX/ATM Devices

The AF network control organizations coordinate NM functions with DISA personnel, but do not directly manage the DISA NIPRNET, SIPRNET, or Integrated Digital Network Exchange/ Asynchronous Transfer Mode (IDNX/ATM) devices.

4.4.2. AF Service Delivery Point (SDP) Router

The AF SDP router is connected directly to the DISA NIPRNET router. The router's primary functions are to provide an entry/exit point to the NIPRNET, route TCP/IP-based network traffic, and to serve as the first line of defense in the AF layered defense strategy. The AFNOC manages the AF SDP router and the NCCs can monitor the device. See the Information Protection Architecture for details.

4.4.3. External Hub

This device is managed by the NCC. Its primary purpose is to provide a connection point for the ASIM and Profiler devices. The device may or may not support SNMP agents.

4.4.4. External Router

The external router provides protection of the base network perimeter and consolidates remote access to internal base resources. See the Information Protection Architecture for additional detail.

4.4.4.1. External Router Management

NCC controllers manage the external router via TELNET (at risk for components outside the firewall), CiscoWorks, and/or HP OV NNM. These NMS components provide full FCAPS functionality to manage this device. NMS functions relative to the external router include: setting service parameters (e.g., committed access rate (CAR), Weighted Random Early Detection (WRED), and Weighted Fair Queuing (WFQ)) to apply precedence by IP address, application, or specific user.

4.4.4.2. External Router Security

An access control list (ACL) only allows authorized NCC controllers to configure, inventory (map), isolate and correct faults, and monitor performance of the external router using the NMS. NOSC and AFNOC controllers are granted read-access rights and can negotiate write-access permissions according to AF and MAJCOM policies and secure mode-of-operations capabilities. Security management is well-defined in the Information Protection Architecture. Air Force Special Security Instruction (AFSSI) 5027 prohibits inbound and outbound SNMP traffic from transiting the security perimeter. However, if required, outbound SNMP traffic from a specified (internal) management system to a specified list of (external) systems being managed, can be permitted. IP address-based packet filtering can be used to restrict outbound traffic.

4.4.5. External Switch

The external switch is installed between the external router and the firewall, providing connectivity for the NMS/BIP components. See the Information Protection Architecture for additional details. NCC controllers manage the external switch via TELNET, CiscoWorks, and/or HP OV NNM. These NMS components provide full FCAPS functionality to manage the external switch. NOSC and AFNOC controllers negotiate access.

4.4.6. Firewall

The firewall, primarily an Information Protection tool, provides boundary protection by selectively identifying and denying unauthorized access. See the Information Protection Architecture for additional detail on how the firewall provides its services. As a managed object, the firewall supports full FCAPS functionality. NCC Network Defense Controllers (Information Protection Operators) use NMS workstations (via TELNET) and/or a direct-connected workstation to manage the firewall. NCC controllers map the firewall manually, then collect, correlate and assess, and report status using HP OV NNM, UNIX performance monitoring commands, and SNMP MIB information. NCC network defense controllers work with Air Force Information Warfare Center (AFIWC) personnel and NOSC/AFNOC network defense controllers to ensure the firewall configuration contains the latest ACLs, filters, and patches.

4.4.6.1. Unprotected SNMP Traffic

AFSSI 5027 prohibits unprotected SNMP traffic, inbound or outbound, from flowing across the firewall. Unprotected SNMP get/set operations that modify or alter the configuration of a managed object external to the firewall are not permitted between the NMS and the managed object. SNMP traps must not trigger automatic processes on external managed objects. Traps can be used to report faults and anomalies.

4.4.6.2. Protected SNMP Traffic

Protected SNMP traffic is authorized. Protected SNMP is defined as specific controlled devices (internal NMS to external list of devices) with filtering mechanisms applied. SNMP community strings do not use the default "public" on external managed objects, the NMS, or internal managed objects. Protected SNMP traffic is collected, compiled, analyzed, reported, and disseminated using NMS tools and electronic messaging systems. For the low speed architecture, the firewall will be one or more application gateways, which provide the capability to proxy, filter, log, translate IP addresses, and/or act as a server for all required protocols and services flowing across the base gateway. Devices external to the firewall can be "managed," but should be limited to fault monitoring, not "fault fixing."

4.4.6.3. Inbound SNMP Traffic

Access lists deny inbound SNMP and ICMP traffic at the external router to prohibit external SNMP probes from obtaining network information.

4.4.6.4. Outbound SNMP Traffic

Except for specified hosts, outbound SNMP traps are also denied at the external router. Access to external devices is limited to internal NMS by a SNMP access list.

4.4.7. Internal Switch

The internal switch connects all demilitarized zone (DMZ) components on the internal side of the firewall according to their respective DMZ functions. The internal switch is identical to the external switch, except for location in the DMZ. It provides connectivity between the NMS/BIP system components via UTP Cat-5 cabling and is located in the NMS trusted subnet. NCC controllers manage the internal switch via TELNET (at risk), CiscoWorks, and/or HP OV NNM. These NMS components provide full FCAPS functionality to manage this device. NOSC and AFNOC controllers negotiate access.

4.4.8. Internal Router

The internal router provides the last layer of defense in the Information Protection Architecture. The internal router provides base boundary protection by providing a last line-of-defense for the base networks against an external attack. As pertains to NM, NCC controllers manage the internal router using TELNET, CiscoWorks, and/or HP OV NNM. These NMS components provide full FCAPS functionality to manage this device. Internal router management includes setting Quality of Service (QoS) parameters (e.g., committed access rate (CAR), Weighted Random Early Detection (WRED), and Weighted Fair Queuing (WFQ)) and applying precedence by IP address, application, or specific user. NOSC and AFNOC controllers negotiate access.

4.4.9. Domain Name Service (DNS) Address Server

A simple DNS provides host name to IP address mapping (forward lookup) and IP address to host name mapping (reverse lookup). Without a DNS, users would have to use IP addresses to connect to remote or local hosts. The DNS is a system of servers strategically placed to provide complete DNS services.

4.4.9.1. Split DNS Operation

Split DNS is a direct result of a firewall installation. The firewall isolates the internal private network from the external public network. Each network requires a DNS to answer requests originating from private and public networks. The internal and external networks share the same domain name (e.g., scott.af.mil) and both have primary and secondary name servers, which can never exchange information with one another. The DNS components consist of primary and secondary, external and internal DNS servers that are connected via the internal and external routers, switches, and sidewinder firewall.

4.4.9.2. External DNS Server

The External DNS server software includes Lucent QIP Enterprise Server with Integrated Database, Remote Server with QDNS and QDHCP, both running on Win NT 4.0 Server with BIND 8.0 enhancements. (Under the CITS program, the AF has an unlimited use enterprise license for Lucent QIP. Contact the CITS PMO for additional information.) The external primary DNS server functions as a remote external secondary DNS server for another base. Hence, there are two external secondary DNS servers--one located off-site at another base and the other located on the external interface side of the local Sidewinder firewall. The primary external DNS is connected to the external switch and provides DNS for all traffic entering the base from the NIPRNET, dial-in services, and other outside connections. The external DNS contains records for only those components considered absolutely essential (e.g., itself, the slave name server, the firewall, external public web server, external FTP server, mail records). Records for hosts or IP addresses for any internal networked resources are not contained on the external DNS server. Limiting the DNS records on the external servers to only those components accessible to outside connections, hides the number, structure, names, and addresses of internal resources from the external public network. Support for external DNS does permit information exchange with public resources through the firewall for communication with internal network resources, when necessary.

4.4.9.3. Internal DNS Server

The Internal DNS server software includes Lucent QIP Enterprise Server with Integrated Database, Remote Server with QDNS and QDHCP, both running on Win NT 4.0 Server with BIND 8.0 enhancements. The primary and secondary internal DNS servers are configured with the host names, IP addresses, mail records, and aliases for the zone for all internal networked resources. The internal interface side of the Sidewinder firewall is configured as the internal secondary DNS server. The primary internal DNS sends a query to the firewall for processing when the internal DNS server can not resolve the DNS lookup. The firewall caches the answer and sends the IP address back to the internal DNS. Only unresolved DNS requests are passed to the secondary internal DNS server located on the internal interface of the firewall.

4.4.9.4. DNS Management

NCC controllers use two NMS workstations to manage the primary DNS servers and the applicable FCAPS functions. The secondary external DNS (Sidewinder) is managed via the Sidewinder workstation. The secondary external off-site DNS is managed by the servicing NCC controllers. Each DNS device supports FCAPS functionality by implementing MIBs. NCC controllers can TELNET to the device and use HP OV NNM and Win NT 4.0 Performance Monitor.

4.4.10. Remote Access Server (RAS)

The RAS equipment is installed in the DMZ on the external side of the firewall via the external switch. It is primarily a component of the Information Protection Architecture. It is included here as a managed object. The RAS consists of two main components, the communications access server and an authentication security database server.

4.4.10.1. RAS Communications Server Management

A communications server exists at each NCC. AFNOC and NCC controllers co-manage the existing remote access servers (i.e., RADTAC Terminal Access Controller Access Control System Plus (TACACS+)) via TELNET. NCC controllers manually discover the device using HP OV NNM and use check performance with Win NT Performance Monitor. NOSC controllers negotiate access.

4.4.10.2. RAS Administration

NCC controllers are granted access by the authentication server before logging into and administering the communications server. Controllers can also log in using a local user name and password, which is kept at the access server. Local user name authentication enables administrators to gain access to the communications server for network troubleshooting or emergency configuration when the authentication security server is not available.

4.4.11. World Wide Web (WWW) Public Access Server

A WWW public access server is connected to the external switch to provide web-based information to the public. Some government systems are connected to the external switch because the systems cannot safely operate through the firewall.

NCC controllers manage the WWW public access server via TELNET, Netscape Proxy Server, Netscape Administration Server, HP OV NNM, and Win NT Performance Monitor. Netscape Navigator is used to manage the Netscape Proxy Server. The Netscape Administration Server is configured to allow only administration from this workstation.

4.4.12. Caching Proxy Server

A Caching Proxy Server works with the firewall to provide faster WWW and File Transfer Protocol (FTP) services to internal base customers. Access speed is shortened by caching the content of frequently visited sites and by reducing the amount of inappropriate non-business oriented WWW traffic.

4.4.12.1. Proxy Server Management

NCC controllers manage the Caching Proxy server via TELNET, Netscape Proxy Server, Netscape Administration Server, HP OV NNM, and Win NT Performance Monitor. Netscape Navigator is used to manage the Netscape Proxy Server. The Netscape Administration Server is configured to allow only administration from this workstation.

4.4.12.2. Proxy Server Operation

The WWW Proxy Server restricts user network access to selected, identified, and appropriate Internet WWW Uniform Resource Locators (URLs). NCC controllers can use Netscape Proxy Server 2.5 software to block certain unsuitable sites from being accessed. A filter list includes sites deemed anti-productive to a working environment (e.g., sexually explicit material, illegal drugs, online gambling, and entertainment).

4.4.12.3. Proxy for Web Hypertext

The firewall is configured to only accept Hypertext Transfer Protocol (HTTP) connections from the proxy server. The proxy server serves as a single outgoing HTTP source to the external network. The proxy server is configured to log end-user activity, provide filtering either by user or URL resource, as well as perform MIME and JAVA script filtering and virus scanning.

4.4.12.4. Proxy Server Port Assignment

The proxy server uses two port numbers, one for the proxy server itself, and another for the administration server which is set to port 8081 by default. Standard port numbers have not been selected for proxy server use. No two-proxy servers can use the same port. Common practice indicates that proxy servers usually use port 8000 and/or 8080.

4.4.13. Network Time Protocol (NTP) Server

The Spectracom NetClock/Global Positioning System (GPS) Master Clock works with the Sidewinder firewall and the NMS server to provide synchronized clock signals to network clients. The Sidewinder and NMS servers are configured as NTP servers; externally generated NTP is blocked on the firewall.

4.4.13.1. NTP Server Operation

Full FCAPS functionality is provided by the NMS server, NMS workstation, Win NT Performance Monitor, and TimeServ server, which the NCC controllers use to manage the system. Time Service for Windows NT is installed on the NMS server and has two primary goals:

- The system time of Windows NT should be accurately set from a variety of sources.
- System time must be synchronized between multiple machines on a LAN.

4.4.13.2. Network Time Synchronization

To easily synchronize the time, TimeServ can access the time from other Windows NT machines or many other machines running networking software from Microsoft. A machine can synchronize from a primary source (one server or a list of specific servers), or a secondary source.

A secondary source is defined as a machine within a domain which sets the "timesource" bit. Another feature in TimeServ allows setting this bit on a Windows NT machine.

4.4.14. Other Servers/Workstations/Peripherals/Applications

Each site has a wide variety of organizational servers, end user desktop workstations, peripherals, and applications--too many to enumerate here. The significant factor is some objects support NM functions while others do not. Optimally, the non-manageable objects will eventually be replaced with manageable objects. The end goal is to provide end-to-end network management that fully supports the Air Force's information assurance goals. The ability to monitor and manage performance and usage (FCAPS) from the desktop-level through the network to the recipient of the information is necessary to obtain these information assurance goals.

4.5. NETWORK MANAGEMENT TOOLS

The standard AF NMS/BIP system delivered multiple products to perform NM and base information protection. Each network control organization and the applicable AF NMS tools is required to conduct NM across their respective AOR are listed in the table below. The NOSCs currently are MAJCOM developed and the need to standardize them will be addressed in future iterations of this architecture as the Enterprise Management Capability CONOPS is developed. Tool selection and location is subject to change as a result of the enterprise network management business process improvement actions.

Table 4-1. NMS Tools to Network Organization Matrix

Component	Description	FCAPS Function(s) Supported	NCC	NOSC	AFNOC	NOTES
SDP Router	Provides service delivery point demarcation between NIPRNET/SIPRNET and the base external router.	FULL			**X**	3
External Router	Provides 1st layer of defense for base networks.	FULL	**X**			1
External Switch	Interconnects components residing on the external side of the firewall in the DMZ.	FULL	**X**			1
Firewall	Provides 2nd layer, primary defense for the base networks and secondary external/internal DNS service.	FULL	**X**			1
Internal Switch	Interconnects components residing on the internal side of the firewall in the DMZ.	FULL	**X**			1
Internal Router	Provides 3rd layer of defense for base networks.	FULL	**X**			1
External DNS Server	Provides primary DNS to external base resources; located in the DMZ.	FULL	**X**			2

Table 4-1. NMS Tools to Network Organization Matrix						
Component	**Description**	**FCAPS Function(s) Supported**	**NCC**	**NOSC**	**AFNOC**	**NOTES**
WWW Proxy	Provides primary WWW proxy service to external and internal networked resources; hides internal resources from unauthorized external view.	FULL	**X**			1
NTP Server	Provides time synchronization to all networked devices.	FULL	**X**			1
RADTAC	Provides remote access service.	FULL	**X**		**X**	3
Internal DNS Server	Provides primary DNS to internal base resources; located in the DMZ.	FULL	**X**			2
Phase 2 Switch	Interconnects NMS/BIP servers and workstations located in the NMS trusted subnet.	FULL	**X**			2
TTS Server	Hosts the trouble ticketing system software and interacts with the RDBMS server.	FULL	**X**		**X**	2
RDBMS Server	Hosts the database management system to support the TTS server.	FULL	**X**		**X**	2
NMS Server-0 Manager	Primary function is NM manager. Hosts NM server and client software to manage base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**		**X**	1
NMS Server-0 Collector	Primary function is collector. Hosts NM server and client software to manage base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**		**X**	1
NMS Workstation 0	Primary function is NM. Hosts client software to manage base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	1
Security Workstation 1	Primary function is security. Hosts client software to manage security of base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	1
Internet Security Scanner Workstation 2	Primary function is security. Hosts client software to manage security of base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	1
TTS Workstation 3	Primary function is trouble ticketing. Hosts client software to manage help desk trouble ticketing operations of base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	2

Table 4-1. NMS Tools to Network Organization Matrix						
Component	**Description**	**FCAPS Function(s) Supported**	**NCC**	**NOSC**	**AFNOC**	**NOTES**
	enterprise network, and AF enterprise network.					
TTS Workstation 4	Primary function is trouble ticketing. Hosts client software to manage help desk trouble ticketing operations of base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	2
NMS Workstation 5	Primary function is NM and DNS server management. Hosts client software to manage DNS and NM operations of base domain and subnets, MAJCOM enterprise network, and AF enterprise network.	FULL	**X**	**X**	**X**	2
Laser Printer	Primary function is Help Desk TTS support—prints trouble tickets.	FULL	**X**		**X**	2
Remote Access System	Primary function is to provide dial-in access to network resources. Consists of communications access server and authentication security database server.	FULL	**X**	**X**	**X**	4
Analog Line Multiplexer	Supports RAS dial-in lines.	FULL	**X**	**X**	**X**	4
VPN	TBD					4

NOTES:

1. Installed (NCC & AFNOC only, NOSC is TBD).
2. Installed or installation scheduled (NCC & AFNOC only, NOSC is TBD).
3. Supplied by AFMC/ESC SSG.
4. To Be Determined (TBD).

Table will include NOSC tools in future iterations of this architecture.

Table 4-1. NMS Tools to Network Organization Matrix.

4.6. INFORMATION FLOWS AND EXCHANGES

AF network operations organizations exchange information internally, between each other, and with external agencies. Information is exchanged to provide commanders with a common operating picture of the AF enterprise network environment. The picture is developed by correlating situational awareness (SA), configuration management (CM), and IA information. The root source of this information comes from "raw" FCAPS data monitored, collected, analyzed, processed and reported by the NCCs, NOSCs, and the AFNOC. This section identifies the FCAPS information/metrics the network operations organizations exchange to operate as the Air Force network and as part of the DoD Global Information Grid. The primary organizations

involved are depicted in Figure 4-1. Common FCAPS information exchanges are explained in the remainder of this section.

Air Force Networks Information Exchange

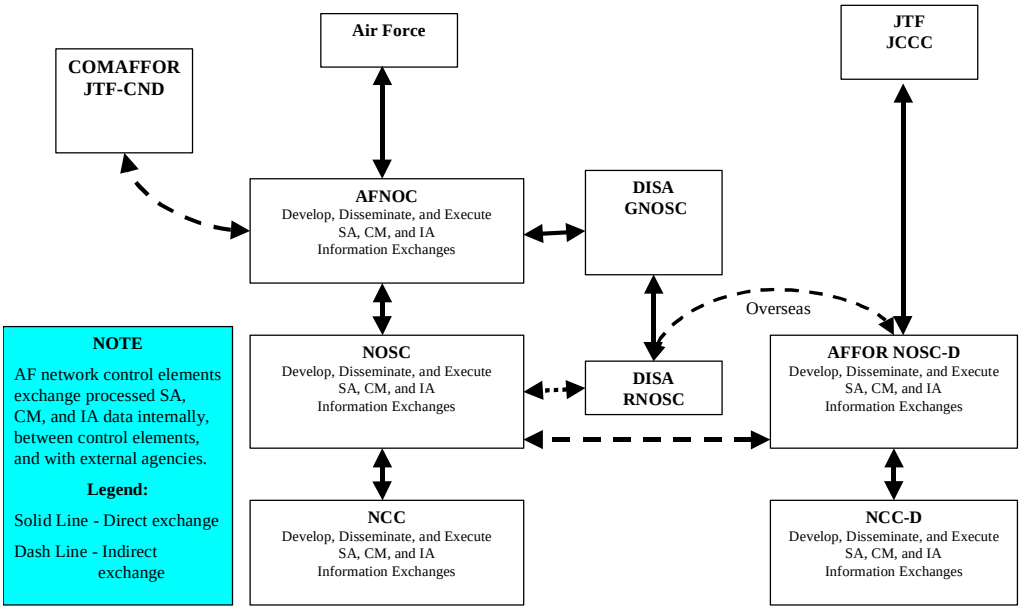

Figure 4-1. Information Exchanges

4.6.1. Situational Awareness (SA)

Network SA is an overall picture of network operations and technical performance. Situational awareness provides a consolidated summary of network status and reports positive and negative trends. Critical metrics on the following areas are reported through situational awareness activities: performance and reliability, capability and availability, configuration management, security, manpower and training, cost, accountability, and planning.

4.6.2. Configuration Management (CM)

CM consists of directing and implementing change. Directing change involves developing and disseminating policies and procedures. Implementing change involves executing policies and procedures by making configuration changes to applications, components, systems, networks, and network services.

4.6.3. Information Assurance (IA)

IA ensures delivery of information to the right person at the right time and place. IA includes network operations, information management, and information protection. Specifically, IA entails optimum delivery of data, availability, reliability, compliance with record storage and disposition instructions, authentication, non-repudiation, and data integrity.

4.6.4. FCAPS Data Exchanges

FCAPS data is regularly exchanged between the various network control organizations. In an effort to control overhead bandwidth consumption, "raw" unprocessed FCAPS data is seldomly exchanged between organizations. Instead, processed FCAPS information is exchanged by using the NMS tools, in conjunction with AF messaging systems.

Table 4-2 identifies which categories of FCAPS data are typically exchanged between network control organizations. For example, the matrix shows that FPS (Fault, Performance, and Security) data is sent from the NCC to the AFNOC, while the AFNOC sends FC (Fault and Configuration) data to the NCC. This matrix is not all inclusive and is meant to be dynamic in that the exchanges take place according to the need at a moment in time.

FCAPS DATA EXCHANGE		**RECEIVING UNIT**						
		AFNOC	**AFCERT**	**NOSC**	**NCC**	**JCCC**	**NOSC-D**	**NCC-D**
SENDING UNIT	**AFNOC**		FS	FPS	FC	Ad Hoc	Ad Hoc	
	AFCERT	S		S	S	Ad Hoc		
	NOSC	FCAPS	S		FCAPS	Ad Hoc	FCAPS	Ad Hoc
	NCC	FPS	S	FCAPS				
	JCCC	Ad Hoc	Ad Hoc	Ad Hoc			FS	
	NOSC-D	FPS		FCAPS		FCAPS		FCAPS
	NCC-D			Ad Hoc			FCAPS	

Table 4-2. FCAPS Data Exchange Matrix

SECTION 5. STANDARDS

This section identifies the technical and/or policy standards that apply to the NMA and are actually implemented by the network control organizations. The matrices below (Tables 5-1 through 5-5) identify standards by FCAPS functional area (Fault, Configuration, Accounting, Performance, and Security Management) and map the standards to service, component, and solution.

This section also identifies emerging standards, those standards currently in draft form or just emerging as standards. These are potential future technical and/or policy standards that may apply to AF network management. As with existing standards, these are also mapped to the service, component, and solution which they are expected to impact.

Table 5-1. FAULT MANAGEMENT STANDARDS MATRIX

SERVICE	COMPONENT	STANDARDS		CURRENT SOLUTIONS	POTENTIAL SOLUTIONS
		CURRENT	EMERGING		
Detect and isolate abnormal network behavior by polling for all infrastructure based components, systems, workstations, applications, SNMP, and extended MIBs. Examine error logs, display and handle alerts (both audible and visual), trace and identify faults, and perform diagnostic tests to a predetermined set of parameters. Define a "fault-detected" notification method (automatically open a job, page a technician, alert at a console, send e-mail, etc.). "Fault-detected" notification must support security extensions for integrity, authentication, and encryption.	Routers, Hubs, ATM and Ethernet Switches, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	RMON2 (RFC-2021), Common Open Policy Service (COPS) draft-ietf-rap-cops-06.txt, RSVP (RFC-1633) , ITU-T X.700	HP OV NNM (excludes desktops, non NT system, and all applications. Also excluding fault isolation and diagnostic test)	
Provide an automated trouble ticketing system that allows the technicians to annotate outages, generate and store reports, and send trouble tickets to appropriate agencies. Allow user level authentication for access to the system. Track/reflect individual making changes to the trouble ticket.	TTS, TTS Distributed Servers, RDBMS Server, Workstations, Printers, Office Automation Software		Open Database Connectivity (ODBC) 3.0 API, X/Open CLI	Remedy ARS	Remedy ARS DSO or equivalent

Table 5-1. FAULT MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Automatically forward trouble tickets based on predetermined escalation schemas and business rules.	TTS			Remedy ARS	Remedy ARS or equivalent
Generate Operational Reports based on a predetermined GENTEXT format for crew commander approval. The format must be compatible with DMS message format.		DII-COE	DII-COE	EMC[2] new requirement	EMC identified point product
ALL reporting provided through a web interface.	WWW Proxy Server	HTML (W3C Rec-html40-19980424), SGML (ISO 8879)	XML (W3C Rec-xml-19990210)	EMC new requirement	EMC identified point product
Transmit Sys logs, MIB data, etc., within an escalated trouble ticket or remotely access the same in a secure fashion.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000), GSS-API (RFC-1508)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), GSS-API Version 2 (RFC-2078)	HP OV NNM	
Use knowledge management to auto-document issues for use by functional end users.	Object Management			No Standard Solution Selected	EMC identified point product
Develop robust reports based on type codes, technicians, functional systems, and user communities.	TTS			Remedy ARS (ad hoc)	Common Remedy ARS schema
Find and disseminate corrective actions.	TTS			Ad hoc (e.g., web sites, ARS, lessons learned)	Common Remedy ARS database

[2] EMC is Enterprise Management Capability initiative

Table 5-1. FAULT MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Automate the logging functions, to include archiving, based on predetermined parameters. Automated logging function will track all changes to tickets by users.	NOS Audit Logs, Back-up software			EMC new requirement	EMC identified point product
Provide automated capability to recover, manage, configure, and monitor system backup.	Tape Backup Tape Library	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213),	SNMPv3 (RFC-2271)	Legato	
Support multiple level help desk operation.	TTS Server, TTS Distributed Servers	Proprietary		Remedy ARS Distributed Server Option (DSO)	

Table 5-1. Fault Management Standards Matrix

Table 5-2. CONFIGURATION MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Automatically discover network components and associated devices, applications, and configurations (both hardware and software) that make up and are connected to the network.	Routers, Hubs, Switches, Workstations, NM Manager, NM Collector, RDBMS Server	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633), ITU-T X.700	HP OV NNM, CiscoWorks	
Automatically map (logical and physical) network components and associated devices, applications, and configurations (both hard-ware and software) that make up and are connected to the network.	Routers, Hubs, ATM and Ethernet Switches, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633), ITU-T X.700	HP OV NNM -- logical map and NT OS only	

Table 5-2. CONFIGURATION MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Automatically collect system configuration information for all network components, such as system administrator data, system mission, criticality, sensitivity, and application of the host.		SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633) , ITU-T X.700	EMC new requirement	SMS, Tivoli, CA Unicenter, TEM, EMC identified point product
Automatically detect and record information concern-ing network components, associated devices, software applications, system parameter settings, and system configurations that make up and are connected to the network.		SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633), ITU-T X.700	EMC new requirement	EMC identified point product
Automatically update and maintain current list of domain names.	DNS Server	DNS (IETF Std 13/RFCs 1034/1035		Lucent QIP	
Automatically install, check, and update network server and end-user software applications.				EMC new requirement	SMS, EMC identified point product
Track the network's current architecture, as well as moves, additions, deletions, changes, and planning network configuration modifications. Allow for manual creation/import/ update of network configuration information.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633), ITU-T X.700	HP OV NNM, CiscoWorks	
Maintain a standard configuration of all network components and report deviations.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations			Axent ESM	SMS

Table 5-2. CONFIGURATION MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Use strong identification and authorization mechanisms including strong password controls, DoD PKI Certificates, and restricting network modification to certain centralized locations/workstations.		ITU-T X.509 (ISO/IEC 9594-8.2)		EMC new requirement	EMC identified point product
Maintain licenses, warranty, and maintenance contracts of applicable components.	License Management			EMC new requirement	SMS, Tivoli, CA Unicenter, EMC identified point product
Allow remote system administrative functions.	Remote System Administration		RADIUS (IETF RFC 2138)		
Provide secure electronic distribution and installation of software and software updates (including remote push based on end station hardware and software configuration).	Electronic Software Distribution			EMC new requirement	EMC identified point product
Provide a detailed assessment of the operational impact of any fault based on known configuration data, such as logical/physical maps, by geographic location and functional user community, and information operational flows.	GEO Spatial Services			EMC new requirement	EMC identified point product
Manage inventory data and be compatible with AF IT asset inventory system.	Inventory Management	GOTS		IPMS	
Maintain SLA requirements with functional communities (QOS).	Office Automation Software				Packeteer

Table 5-2. CONFIGURATION MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Provide on-line documentation to include user manuals, installation manuals, tech orders, and trouble shooting guides.	On-line Reference	X/Open C323, CDE version 1.0		No Standard Solution Selected	
Provide a Graphical User Interface (GUI) capability to allow manual/automatic modification of the configuration data.		X/Open C323, CDE version 1.0	DII COE	EMC new requirement	COTS

Table 5-2. Configuration Management Standards Matrix

Table 5-3. ACCOUNTING MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Provide the capability to collect end user and functional community traffic statistics. Display and print real-time analysis of related interface data.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations			EMC new requirement	EMC identified point product
Track system downtime, manpower impacts and statistics related to trouble tickets and information defense activities.	TTS			Remedy ARS	Remedy ARS DSO
Track cost and accounting information for AF assets and licenses.			ITU-T X.700	EMC new requirement	EMC identified point product

Table 5-3. Accounting Management Standards Matrix

Table 5-4. PERFORMANCE MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Support collection and display of performance data. Report critical performance metrics in standard free-form reports.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633) , ITU-T X.700	HP OV NNM, CiscoWorks (partial solution)	COTS
Perform analysis at selected intervals for applicable components and applications [IAW the AFCA-developed AF Enterprise Network Operations Metrics package, dated 1 Jun 99 (draft)]. This includes: collection of defined metrics on a scheduled basis using standard industry protocols; scheduled and on-demand display of collected statistics and graphic charts and ASCII formats; storage and retrieval of historical data in a variety of intervals to support trend analysis; support roll-up of older historical data; provide WEB access to metrics reports; include statistical analysis functions (e.g., MEAN, MAX, DIST, Percentage over time); and, allow input for correction factors.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633) , ITU-T X.700	HP OV NNM, CiscoWorks (partial solution)	COTS

Table 5-4. PERFORMANCE MANAGEMENT STANDARDS MATRIX					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Perform trend analysis and provide trend analysis reports and graphs at user-defined intervals for applicable components and applications [IAW the AFCA-developed AF Enterprise Network Operations Metrics package, dated 1 Jun 99 (draft)].	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations	SNMP (IETF Std 15/RFC-1157), MIB (IETF Std 17/ RFC-1213), RMON (IETF RFC-1757), ATM ILMI (af-ilmi-0065.000)	SNMPv3 (RFC-2271), RMON2 (RFC-2021), COPS (draft-ietf-rap-cops-06.txt), RSVP (RFC-1633) , ITU-T X.700	HP OV NNM, CiscoWorks (partial solution)	COTS
Dynamically monitor and manage information flow based on all layers of the OSI model and IPS, to include resource allocation between end users, functional communities, protocols and applications.	NM Manager, NM Collector, RDBMS Server, Messaging server, Workstations				COTS
Automatically conduct modeling and simulation to assess performance, capacity and desired threshold.			IEEE 1320.2-1998, standard for Conceptual Modeling Language Syntax and Semantics for IDEF1X97 (IDEF object) and the Unified Modeling Language (UML)		COTS
Sort and file network traffic data based on source, destination IP addresses, and applications.	Profiler	GOTS		Profiler	COTS
Assign/code a corrective action to a performance fault related to a threshold association.				EMC new requirement	EMC identified point product

Table 5-4. Performance Management Standards Matrix

Table 5-5. SECURITY MANAGEMENT STANDARDS MATRIX					
Security management must integrate the existing info protect tools into network management interfaces as well as monitor, deter, detect, isolate, contain, control, report, and recover from intentional or unintentional unauthorized intrusions, abuse, denial of service, and use of Automated Information System (AIS) resources. SM is performed using BIP tools and is described in detail in the Information Protection Architecture. The few SM services that are not explicitly included in the Information Protection Architecture are addressed in this table.					
SERVICE	**COMPONENT**	**STANDARDS**		**CURRENT SOLUTIONS**	**POTENTIAL SOLUTIONS**
		CURRENT	**EMERGING**		
Provide an Operator's Graphical User Interface (GUI) capability. Must provide IPO technicians with a point-and-click interface to remotely configure sensors from their control stations.		X/Open C323, CDE version 1.0	DII COE	EMC new requirement	COTS
Select and configure session captures based on alarm levels, keystroke specificity, or source and destination of the activity.		Proprietary	DII COE	EMC new requirement	COTS
Provide the ability to remotely reconfigure security policy base-wide and enterprise-wide, in response to changes in the “Information Condition" (INFOCON).	NM Console, Managed Objects	Proprietary		EMC new requirement	COTS
Automatically generate and store connection logs to identify the source, destination, type of service, type of protocol, ports used, connection data and time, and other defined information.	Profiler	GOTS		Profiler	COTS
Provide for a controllable playback capability and allow post analysis processing of previously collected data using new analytical criteria or parameters.	NM Collector, Modeling & Simulation tool			EMC new requirement	COTS Modeling & Simulation

Table 5-5. Security Management Standards Matrix

SECTION 6. "FUTURE" SOLUTION

This section looks at the future architecture, covering the 2002-2007 timeframe. Projections indicate the NM arena will grow evolutionarily. NM management tools will gain increased capabilities, particularly in their ability to interpret gathered data. Agents, necessary to manage a network object, will become available for virtually all network devices. Standards will continue to evolve to accommodate the technology changes and the ever expanding scope of the networks. Where appropriate, evolving standards and potential solutions are identified in the Section 5 standards matrices (Table 5-1 through 5-5).

6.1. NMS FUTURE CONSIDERATIONS

Technology's rapid advancement makes it difficult to project exactly what will be available and practical in the network management arena. There are several areas or specific products that will likely be major players in the network management arena. These are discussed briefly in subsequent paragraphs. The intent is not to present a full discussion of each topic, but to serve as a reminder of areas/products to consider.

6.1.1. Modeling and Simulation

Modeling and Simulation (M&S) will bring its capabilities (e.g., planning, fault replication and isolation, optimization) to the NM arena. The basic concept will use a network auto-polling feature to feed configuration information into an established M&S tool (e.g., OPNET) to "auto-generate" a network model. The M&S tool can then be used to achieve many diverse goals. For example, a network office that wielded this tool could feed the AFMC ESC/DIIO Simulation Office information on a scheduled basis. The simulation office could then create up-to-date models for the benefit of the Air Force community.

6.1.2. Manager of Managers

Future products will be able to assimilate the network management information from multiple varied sources and present a comprehensive picture of an entire network. Some commercial products are already available, but their scope is currently limited.

6.1.3. Windows 2000

The widespread deployment of Windows 2000 and the potential use of its Active Directory structure may have extensive impact on network management.

6.1.4. Geographic Information System (GIS) Network Mapping

The potential marriage of GIS with network mapping tools could significantly change network management. The possibility of being able to both logically and physically locate a problem from a central location could enhance maintenance. The availability of this information could enhance planning, allowing engineers to actually "see" the environment they are planning for. These are but small examples of the potential of using GIS systems in network management.

6.1.5. Deployed Environment

Network management of deployed networks is as critical as for fixed-site networks. Consideration must be given to interoperability with other AF network management organizations, as well as with Joint network management organizations.

6.1.6. C2 Networks

Ideally, the AF Enterprise Network Management capabilities should include being able to manage all AF networks. This would include the C2 networks such as GCCS and GCSS. Consideration would have to be given to monitoring versus managing, as C2 programs typically fund their own communications links to ensure their specific requirements are met.

6.2. NMS FUTURE PRODUCTS

The below listed items are provided as potential future solutions, not as recommended products. The items are intended to serve only as examples of the types of products that are anticipated to be needed to continue evolving network management operations.

- BMC Patrol
- Concord Network Health
- HP NetMetrix
- MIL3 OPNET Planner
- HP OpenView Manage X
- APC PowerNet
- SMARTS IP Fault Manager (IPFM)

SECTION 7. "STRATEGIC" SOLUTION

This section looks at the future architecture, covering the 2008 and beyond timeframe. It is largely undetermined at this time, and will be addressed in future iterations of this document. The "strategic" goal is to provide end-to-end network management of all Air Force networks (e.g., classified, unclassified, data, voice, video, imagery, and C2 networks), fully supporting the Air Force's information assurance goals. The ability to monitor and manage performance and usage (FCAPS) from the originator, through the network, to the recipient of the information is necessary to obtain these information assurance goals.

SECTION 8. RECOMMENDED PRODUCTS

The following NMS components, addressed in Section 4: Component, Service, and "Now" Solution, are specified as JTA-AF Recommended Products.

- Hewlett Packard (HP) OpenView (OV) for Windows NT
- CiscoWorks for Windows NT
- Dolch PAC64/Network General Protocol Analyzer
- Spectracom Master Clock and GPS Receiver
- Trouble Ticketing System (TTS) - Enterprise License for Remedy Trouble Ticketing License, includes
  - Remedy Action Request System (ARS)
  - Remedy Distributed Server Option (DSO)
  - Remedy fixed/floating client licenses
- Microsoft SQL Server

APPENDIX 9 - ACRONYMS

ACRONYM	NAME OR PHRASE
ACL	Access Control List
ACM	AFCERT Advisory Compliance Message
AFCA	Air Force Communications Agency
AFFOR	Air Force Forces
AFIWC	Air Force Information Warfare Center
AFNOC	Air Force Network Operations Center
AFSSI	Air Force Special Security Instruction
AIS	Automated Information System
AM	Accounting Management
AOR	Area of Responsibility
ARS	Action Request System
ASIM	Automated Security Intrusion Monitoring
ATM	Asynchronous Transfer Mode
BIP	Base Information Protect
C4ISR	Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance
CAR	Committed Access Rate
CBR	Case Based Reasoning
CES	ATM Circuit Emulation Standard
CGI	Common Gateway Interface
CITS	Combat Information Transport System
CM	Configuration Management
COA	Course of Action
CODEC	Coder-Decoder
COMM & Info	Communication and Information
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CSP	Client Server Protocol
CSU/DSU	Channel Service Unit/Data Service Unit
DII-COE	Defense Information Infrastructure Common Operating Environment

ACRONYM	NAME OR PHRASE
DITCO	Defense Information Technology Contracting Office
DMC	Defense Megacenters
DMI	Desktop Management Interface
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DNS	Domain Name Service
DRU	Direct Reporting Unit
DSO	Distributed Server Option
EMC	Enterprise Management Capability
ESM	Enterprise Security Management
ESM	Enterprise Security Manager
FAB	Field Assistance Branch
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FDDI	Fiber Distributed Data Interface
FM	Fault Management
FTP	File Transfer Protocol
GPS	Global Positioning System
GUI	Graphical User Interface
HD	Help Desk
HP	Hewlett Packard
HSSI	High-Speed Serial Interface
HTTP	Hypertext Transfer Protocol
HUM	Heads Up Message
IA	Information Assurance
ICMP	Internet Control Message Protocol
IDNX	Integrated Digital Network Exchange
IETF	Internet Engineering Task Force
INFOCON	Information Operations Condition
IP	Internet Protocol
IPMS	Information Processing Management System
IPX	Internet Packet Exchange
ISO/IEC	International Standards Organization/ International Electro-technical Commission
ISS	Internet Scanner SafeSuite

ACRONYM	NAME OR PHRASE
ITA	Intruder Alert
ITS	Information Transport System
LAN	Local Area Network
M&S	Modeling and Simulation
MAN	Metropolitan Area Network
MIB	Management Information Base
NCC	Network Control Center
NCC-D	NCC-Deployed
NIC	Network Interface Card
NM	Network Management
NMA	Network Management Architecture
NMS	Network Management System
NNM	Network Node Manager
NOS	Network Operating System
NOSC	Network Operations and Security Center
NOSC-D	NOSC-Deployed
NTP	Network Time Protocol
OC-3	Optical Carrier-3
ODBC	Open Database Connectivity
OPREP	Operational Report
OSIE	Open System Interconnect Environment
OV	OpenView
PBX	Private Branch Exchange
PM	Performance Management
POM	Program Objective Memorandum
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Inexpensive (or Independent) Disks
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Server
RDBMS	Relational Database Management System Server
RFC	Request for Comments
RMON	Remote Network Monitoring

ACRONYM	NAME OR PHRASE
RPC	Remote Procedure Call
RSP	Route Switch Processor
RSVP	Resource Reservation Protocol
SA	Situational Awareness
SAN	System Advisory Notice
SDP	Service Delivery Point
SDPOP	Service Delivery Point-of-Presence
SITREP	Situational Report
SLA	Service Level Agreement
SM	Security Management
SMS	Service Management System
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSG	Standard Systems Group
TACACS+	Terminal Access Controller Access Control System Plus
TBD	To Be Determined
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Theater Deployable Communications
TDY	Temporary Duty
TTS	Trouble Ticketing System
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VIP	Versatile Interface Processor
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WWW	World Wide Web

APPENDIX 10 - NETWORK MANAGEMENT ORGANIZATIONS

The AFNOC, NOSC, and NCC perform AF network management functions. Each of these organizations operates at a different level in the AF network structure; either at the base-level, MAJCOM-level, or AF Enterprise-level.

A2-1. AIR FORCE NETWORK OPERATIONS CENTER (AFNOC)

The AF's top tier of network management is the AFNOC, whose primary role is to provide a consolidated, single view of the Air Force's network. To accurately portray this picture, the AFNOC manages both classified and unclassified network operations and correlates network operations with incident reporting to produce a global situational awareness picture of communications and information assets for the Air Force. The AFNOC monitors changes in communications and information networks, systems, and applications. It performs FCAPS management on combat support networks and mission systems (e.g., Global Command and Control System). AFNOC on-site technicians provide flexible and scaleable levels of service to NOSCs 24 hours per day, 7 days per week.

The Enterprise Network Support Center (ENSC), which is part of the AFNOC, provides a help desk service for CITS NMS/BIP and will be covered in a future iteration of this architecture.

A2-2. NETWORK OPERATIONS AND SECURITY CENTER (NOSC)

MAJCOM and Air Force Forces (AFFOR) commanders exercise command and control over their respective regional enterprise networks and mission systems via the NOSC. The regional enterprise network is a mission critical weapon system. The NOSC gives commanders visibility into the network to achieve operational objectives. Every MAJCOM will have a NOSC to provide commanders a real-time presentation of their network forces. Some MAJCOMs will establish NOSC-deployable (NOSC-D) at predetermined Numbered Air Forces based on mission need. Within their enterprise, each MAJCOM NOSC generates an enterprise situational awareness picture and manages network configuration. The NOSC serves as the conduit between the AFNOC and the NCC. NOSC on-site technicians provide flexible and scaleable levels of service to NCCs 24 hours per day, 7 days per week.

A2-3. NETWORK CONTROL CENTER (NCC)

Wing commanders exercise command and control over their fixed base or deployed site networks and systems via the NCC. The NCC generates the local situational awareness picture and manages the local network configuration. They perform FCAPS management on combat and combat support networks and mission systems. Network management operations are performed on video, imagery, data, and sensor networks supported by base/site long-haul links, trunks, and circuits. An NCC provides these services for a fixed base, while a NCC-D provides the same services for a theater air base or other deployed site. NCC technicians provide flexible and scaleable levels of service to functional system administrators, workgroup managers, and users 24 hours per day, 7 days per week.

APPENDIX 11 - ENTERPRISE NETWORK FCAPS CORE OPERATIONS

A3-1. CORE OPERATION AREAS

Network control organizations conduct FCAPS functions in six core operational areas: Event Management, Network Assistance, Infrastructure Management, Information Flow Management, Network Core Services, and Network Defense. The network management organizations, enterprise network core operations, FCAPS roles and responsibilities, applicable NMS tools, and information exchanges are key pieces of any network management architecture. The combination of these operational factors, this architecture, and applicable NMS tools interrelate to form the NMA "Now" solution.

The AFNOC, NOSC, and NCC all perform similar functions with a different scope of operations. Each network operations organization must perform the following six core operations.

A3-2. EVENT MANAGEMENT

A network event is any incident (security, performance, or fault related) affecting network operational availability. Event management is the process of identifying and reacting to network events and restoring network operational availability. Help desk technicians, functional system administrators, workgroup managers, and event managers incorporate various event management tools for event correlation to provide situational awareness to operational commanders. Event management includes the analysis and correlation of network events to produce Operational Reports (OPREPs), Situational Reports (SITREPs), and Information Operations Condition (INFOCON) status changes indicating potential network probes, attacks, and degradations. Individuals performing event management gather and analyze statistical data to identify potential problem areas and effect solutions.

A3-3. NETWORK ASSISTANCE

Each network operations organization provides network assistance to lower tier organizations (in the case of the NCC, to workgroup managers, functional system administrators, and users). Help desk technicians and event managers field all trouble calls, prioritize workload, and escalate problems they cannot resolve to subject matter experts--military or commercial--as necessary. If mission requirements dictate, the network operations organization coordinates on-site technical assistance. Individuals performing network assistance track all trouble calls to final resolution, and log the problem and final resolution in a central database repository. The enterprise management tool set is used to query the repository to identify common network problems and trends. Network operations organizations freely exchange standard problem resolutions, best practices, tips-of-the-trade, and lessons-learned to avoid redundancies.

A3-4. INFRASTRUCTURE MANAGEMENT

Network operations organizations manage, troubleshoot, and monitor AF networks. Network managers and enterprise controllers implement and maintain operational procedures, as well as manage network changes and installations. Network status reports such as performance metric, situational awareness, change management, and information assurance are submitted to appropriate authorities. Ad-hoc queries that correlate the information needed for network assistance and course of action (COA) development are also performed by network managers.

Detailed infrastructure mapping, analysis, and management are conducted to make recommendations for resource allocation and prioritization to the appropriate authorities. Network managers and enterprise controllers respond to detected network faults and reported outages at the time of Network Assistance referral.

A3-5. INFORMATION FLOW MANAGEMENT

Operations for conducting information flow management are similar to those for infrastructure management, except the focus is on logical flow of information and quality of service instead of performance of physical devices. Not every packet, cell, or frame traversing the network has the same priority; information flow management ensures the optimal delivery of data to support line-of-business applications. Network managers and enterprise controllers assess equipment configuration, capacity, and performance to ensure information flow reliability and effectiveness. Resulting assessment reports are used as the basis for additions and changes to network infrastructure, network device configuration, and network usage policies.

A3-6. NETWORK CORE SERVICES MANAGEMENT

Network administrators and enterprise controllers configure, install, and manage services to support organizational mission requirements. Examples include NIPRNET/SIPRNET access and Domain Name Service (DNS) management.

A3-7. NETWORK DEFENSE OPERATIONS

Network operations organizations perform network defense by operating intrusion detection and vulnerability assessment tools on AF networks. Information protection operators and network defense controllers execute internal network defense ROE, countermeasures, and other courses of action in response to command direction and INFOCONs. Network operations organizations direct and assist subordinate AF network operations organizations to execute equivalent actions to control malicious events and perform AFCERT Advisory Compliance Message (ACM) follow-up. Network operations organizations receive consolidated intrusion detection reports and data, assess the compiled data, and report the results to the appropriate command authorities.

A3-8. FCAPS ROLES AND RESPONSIBILITIES

Table A3-1 contains the FCAPS roles and responsibilities for the AFNOC, NOSC, and NCC. The table is organized by FCAPS category (i.e., FM, CM, AM, PM, and SM), subcategory, description, and network control organization.

Table A3-1. FCAPS Roles & Responsibilities to Network Organization Matrix					
FCAPS			**Applicability**		
Category	**Sub Category**	**Description**	**NCC**	**NOSC**	**AFNOC**
FM	Detection	Respond to escalated trouble calls from NOSCs and Direct Reporting Units (DRUs) (Help Desk Operations)	**X**	**X**	**X**
		Respond to failures and degradations detected by AFNOC tools tracking	**X**	**X**	**X**
		FAB maintain enterprise problem resolution database (Remedy ARS)	**X**	**X**	**X**
		Immediate feedback and information dissemination services to NOSCs	**X**	**X**	**X**
		Feedback on types of calls and associated trends to each NOSC and SPO	**X**	**X**	**X**
		Feedback on AF Enterprise faults as provided by automated tools and the impact to operational missions	**X**	**X**	**X**
	Resolution	Coordinate with DISA/Defense Information Technology Contracting Office (DITCO) to ensure proper activation and restoration of DoD services	**X**	**X**	**X**
		Coordinate and provide on-site support when required and requested by the NOSC and DRUs	**X**	**X**	**X**
		Coordinate with commercial vendors on commercial-off-the-shelf (COTS) products	**X**	**X**	**X**
		Coordinate with NOSCs and affected NCC on the status of the resolution	**X**	**X**	**X**
		Coordinate with DISA/DITCO ensuring proper activation and restoration of DoD priority circuits	**X**	**X**	**X**
CM		Provide network baseline configuration software support, maintain baseline media library, and distribute network computer products	**X**	**X**	**X**
		Perform and plan capacity adjustments, interoperability testing, performance modeling, and vulnerability assessment for changes to the baseline	**X**	**X**	**X**
		Monitor the configuration, control configuration changes, and analyze utilization of wide area networks (WANs), both unclassified and classified	**X**	**X**	**X**
		Obtain and maintain AF-wide site licenses for all AF units through a central software control board	**X**	**X**	**X**
		Provide AF-wide IP address management, validating usage, structure, and requirements for AF bases	**X**	**X**	**X**

Table A3-1. FCAPS Roles & Responsibilities to Network Organization Matrix					
FCAPS			**Applicability**		
Category	**Sub Category**	**Description**	**NCC**	**NOSC**	**AFNOC**
CM		Manage the AF enterprise DNS and Reverse Address Resolution Protocol (RARP)	**X**	**X**	**X**
		Interface with source agencies for line-of-business applications performance for enterprise network management	**X**	**X**	**X**
		Provide contingency and exercise support, as required	**X**	**X**	**X**
AM		Use end-to-end network performance metrics to advocate for enterprise information assurance improvements and modernization	**X**	**X**	**X**
		Determine Total Cost of Ownership (TCO) for systems utilizing the enterprise network	**X**	**X**	**X**
PM		Monitor and archive AF enterprise information flow characteristics (i.e. bandwidth and traffic usage) for AF SDPs, and provide real-time view to the NOSCs	**X**	**X**	**X**
		Provide PMOs feedback on performance impact of program software and hardware to enterprise network	**X**	**X**	**X**
		Implement, coordinate, reports, and track Information Condition (INFOCON) statuses	**X**	**X**	**X**
		Manage and control the IP based access control lists (ACL) residing on SDPs	**X**	**X**	**X**
SM		See the Information Protection Architecture for details	**X**	**X**	**X**

Table A3-1. FCAPS Roles & Responsibilities to Network Organization Matrix